					[Insert Registered Legal Entity Name Here]							
Document number: P11					Document Title: **User Account and Privilege Management Policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	Clause 6.1.3, Clause 8.1	
ISO/IEC 27002:2022	Controls 5.15-5.18	
NIST SP 800-53 Rev.5	AC-1, AC-2, AC-5, AC-6, IA-2-IA-5, AU-2, AU-12	
EU GDPR	Articles 5(1)(f), 32; Recital 39	
EU NIS2	Articles 21(2)(a, d), 21(3)	
EU DORA	Articles 5, 9	
COBIT 2019	DSS01, DSS05, APO13	

1. Purpose

1.1 This policy establishes mandatory controls for the management of user accounts and privileges across all information systems and services. It ensures that access to organizational resources is granted based on validated identity, role necessity, and the principles of least privilege and separation of duties.

1.2 It supports the organization's commitment to information security by implementing structured, auditable processes for account provisioning, privilege assignment, usage monitoring, and account revocation.

1.3 This policy is critical for reducing the risk of unauthorized access, privilege misuse, insider threats, and non-compliance with applicable regulatory frameworks.

2. Scope

2.1 This policy applies to all employees, contractors, third-party service providers, consultants, and other individuals granted access to the organization's IT resources, applications, or data.

2.2 It governs all systems and environments where user authentication and access control mechanisms are applied, including but not limited to:

2.2.1 Enterprise applications and databases

2.2.2 Cloud platforms and SaaS environments

2.2.3 Operating systems and administrative consoles

2.2.4 Remote access tools and VPNs

2.2.5 Identity and access management (IAM) systems

2.3 The policy encompasses both standard and privileged user accounts, and includes controls over:

2.3.1 Account creation, modification, and deactivation

2.3.2 Privilege escalation and delegation

2.3.3 Session control and monitoring

2.3.4 Authentication methods and credential management

3. Objectives

3.1 To ensure all user accounts are uniquely identifiable, properly authorized, and assigned only after formal validation of need.

3.2 To implement least privilege principles and prevent unnecessary or excessive access by enforcing strict controls on privileged account issuance and usage.

3.3 To require timely updates to account status based on employment or role changes, including immediate deactivation upon termination.

3.4 To enable proactive detection and remediation of dormant, misused, or unauthorized accounts via logging, reviews, and automation.

3.5 To maintain alignment with ISO/IEC 27001:2022 and associated standards, and to satisfy obligations under relevant legal and regulatory frameworks such as the GDPR, NIS2, DORA, and COBIT 2019.

4. Roles and Responsibilities

4.1 Chief Information Security Officer (CISO)

4.1.1 Owns this policy and ensures its enforcement across the organization.

[…….]

11. Reference Standards and Frameworks

This policy is aligned with globally recognized cybersecurity standards and regulatory frameworks that mandate secure identity, access, and privilege management as a core component of organizational information security.

ISO/IEC 27001:2022

Clause 6.1.3 - requires organizations to determine, evaluate, and treat information security risks—making access and privilege management a formal, risk-based control embedded within the ISMS planning process.

Clause 8.1 - Operational Planning and Control: Reinforces implementation of technical and procedural safeguards that govern user and privileged access.

ISO/IEC 27002:2022 - Controls 5.15 to 5.18

Control 5.15 - User Access Management: Supports formal processes for account provisioning, access authorization, and periodic review of access rights.

Control 5.16 - Identity Management: Establishes identity uniqueness, lifecycle controls, and secure authentication enforcement.

Control 5.17 - ensures that the allocation and use of privileged access rights are strictly controlled, traceable, and aligned with the principle of least privilege throughout the user account lifecycle.

Control 5.18 - Privileged Access Rights: Fully addressed through role-based privilege assignment, auditing, and elevated access approval requirements.

These controls guide structured implementation of account registration, de-registration, privilege separation, and use of authentication information. The policy enforces identity lifecycle governance, just-in-time access, and elevated session monitoring to prevent unauthorized system use.

NIST SP 800-53 Rev.5

AC-1 (Access Control Policy) and **AC-2** (Account Management): Mapped through policy mandates for access approvals, role mapping, and user account auditing.

AC-5 (Separation of Duties) and **AC-6** (Least Privilege): Fulfilled through privilege restriction, job-role alignment, and dual-approval for high-risk tasks.

IA-2 to IA-5 (Identification and Authentication): Enforced via strong authentication mechanisms, credential lifecycle rules, and MFA requirements.

AU-2, AU-12 (Audit Logging and Analysis): Addressed through session recording and privileged activity monitoring across sensitive environments.

EU GDPR (2016/679)

Article 32 - Security of Processing: Requires access controls and identity verification mechanisms to protect personal data. Fulfilled by mandating account approvals, privilege reviews, and strong authentication safeguards.

Article 5(1)(f) - Integrity and Confidentiality: Ensures personal data is accessed only by authorized users with legitimate roles, reinforced by account management enforcement.

Recital 39: Calls for clear access limitation and accountability—this policy supports full traceability of user identities and privilege assignments.

EU NIS2 Directive (2022/2555)

Article 21(2)(a, d): Requires entities to enforce access management policies and secure handling of credentials and privileged sessions, supported through this policy's provisioning, monitoring, and exception controls.

Article 21(3): Promotes access discipline and strong identity assurance in critical sectors, met through the use of unique IDs, RBAC, and time-restricted elevated access.

EU DORA (2022/2554)

Article 5 - ICT Governance and Control: Mandates formalized processes for ICT user management, covered through documented provisioning, deactivation, and exception handling.

Article 9 - ICT Risk Management: Directs organizations to secure systems through access restrictions and monitoring, addressed via MFA, privileged access logging, and centralized reviews.

COBIT 2019

DSS01 - Managed Operations: Promotes enforcement of standardized operational controls, including user account lifecycle management and access documentation.

DSS05 - Managed Security Services: Reflects secure administration of user and system privileges, supporting risk mitigation through least privilege and audit trail validation.

APO13 - Managed Security: Requires access governance across digital assets, fulfilled through formalized account and role authorization practices with periodic review mandates.